Reunião CSI- 10/05/2022

1 Participantes

Hebert Pinheiro, Antonio Ferreira, Gualter Gonçalves, Leana Neves, Gustavo Adriano, Daniele Cavaignaic, Wellington Silva, Alysson Cristiano

2 VPN

2.1 Definição

2.1.1 Rede Privada Virtual

2.1.2 Utiliza meio público (internet) para criar um túnel privado

2.1.3 Ponto de Acesso externo para rede interna

2.1.4 Principal meio de acesso para atacantes (TRE-RN/TSE/GEDAI)

2.2 REVISÃ0/ALTERAÇÃO DA NORMA DE CONTROLE DE ACESSO EM 2021

2.2.1 Acesso à VPN por padrão será bloqueado de segunda a sexta-feira durante a noite (a partir das 22h até às 6h da manhã). As exceções serão tratadas pelo DG;

2.2.2 A solicitação deverá ser feita pelo Gestor Máximo da Unidade através de SEI direcionado para a SERED;

2.2.3 A revalidação do acesso ocorrerá em meses fixos (janeiro, abril, julho e outubro) para facilitar a operacionalização por parte da Sered devido a limitações da ferramenta de VPN. Nestes meses os acessos serão bloqueados sendo necessário envio de SEI solicitando a renovação do acesso;

2.2.4 O fiscal de contrato pode solicitar acesso temporário VPN para prestadores de suporte enviando SEI direcionado à COINF devendo o serviço ser acompanhado pelo fiscal. Esse acesso não poderá ultrapassar 12h de acesso contínuo;

2.2.5 Para que ocorra a autenticação da conta de usuário atualmente é enviado um token (código) para o email institucional. Ocorre que a senha de email da conta de usuário é a mesma do e-mail institucional e, portanto, se a conta de usuário for comprometida o atacante terá acesso ao e-mail institucional e poderá recuperar o token para acessar a VPN. A modificação proposta é que seja enviado o token para um email externo à Justiça Eleitoral que possui senha diferente da senha institucional.

3 Ransomware

3.1 Definição

3.1.1 Torna inacessível dados armazenados

3.1.2 Exige pagamento de resgate (bitcoin)

3.1.3 Principal tipo de ataque

3.2 Tipos

3.2.1 Locker

3.2.1.1 Impede acesso ao equipamento

3.2.2 Cripto

3.2.2.1 Impede acesso aos dados